IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	Anthony L. Fontaine *et al.*	**Examiner:**	FISCHER, Andrew J.
Application No.:	10/033,716	**Group Art Unit:**	3621
Filing Date:	December 27, 2001	**Confirmation No.**	8636
Notice of Appeal:	May 20, 2008	**Docket No.**	83336.0559
Title: REMOTE ACCESS VERIFICATION ENVIRONMENT SYSTEM AND METHOD		**Customer No.**	66880

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

The following Appeal Brief is submitted pursuant to the Notice of Appeal dated May 20, 2008 for consideration by the Board of Appeals and Interferences. 37 C.F.R. § 41.37.

(i) REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: Bally Gaming International, Inc., 6601 S. Bermuda Road, Las Vegas, Nevada 89119.

(ii) RELATED APPEALS AND INTERFERENCES

There are no prior or pending appeals, interferences, or judicial proceedings known to the appellant, the appellant's legal representative, or the assignee which may be related to, directly affect, or be directly affected by, or have a bearing on the Board's decision in this pending appeal.

(iii) STATUS OF CLAIMS

Claims 1, 2, 6-8, 11-13, 15, 16, 18-34, 48, 49, 52-55, 58-60 and 62-84 are pending. Claims 77-84 have been withdrawn. Claims 1, 2, 6-8, 11-13, 15, 16, 18-34, 48, 49, 52-55, 58-60, and 62-76 have been rejected and are now being appealed.

(iv) STATUS OF AMENDMENTS

No amendments have been filed subsequent to the final rejection mailed March 20, 2008.

(v) SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1:

A system for enabling remote access (p.3, ll. 22-23) to an application server (p. 3, l. 24), the system comprising:

a means for enabling a user to request remote access to the application server (p. 3, ll. 29-30);

a gaming card having security data for identifying the user (p. 16, ll. 17-19);

an access server (p.3, l. 28), for receiving and processing a request for access to the application server (p. 3, ll. 27-29) from the means for enabling a user to request remote access to the application server (p. 3, ll. 29-30), the access server adapted to be located remote from the user's geographic location (p. 3, l. 30);

a card reader (p. 17, ll.19-21) connected to the means for enabling a user to request access to the application server (p. 3, ll. 29-30) at the user's geographic location (p. 17, ll. 21-24), wherein the card reader (p. 17, ll.19-21) includes a time out feature (p. 17, ll. 21-24) that prompts the user to insert the gaming card into the card reader at an appropriate time to verify that the user is physically present at the user's geographic location;

an authenticator for authenticating the geographic location of the user responsive to receipt of a processed request from the access server (p. 3, l. 30 – p. 4, l. 1), the authenticator including a challenge and response system (p. 4, ll. 19) for authenticating the geographic location of the user and verifying an identity of the user based on the security data (p. 4, ll. 19-20), wherein the verifying the identity of the user includes issuing a challenge based on the security data (p. 4, l. 21), and wherein the authenticator is adapted to be connected to the access server (FIG. 1; p. 8, ll. 26-27);

means for interconnecting the access server and the authenticator (FIG. 1; p. 4, l. 27); and

a first number authenticating system (p. 9, l. 27- p. 10, l. 2), wherein the first number authenticating system provides anti-circumvention protection that determines a geographic location of an originating number to prevent the user from connecting to the access server from a geographic location other than the user's geographic location (p. 9, l. 27- p. 10, l. 2), and wherein

the first number authenticating system relies on user input (p. 5, ll. 14-15; p. 17, ll. 13-14) and does not rely on GPS (p. 4, ll. 12-14).

Independent Claim 30:

A system for enabling remote access (p. 3, ll. 22-23) to an application server (p. 3, l. 24), the system comprising:

a means for enabling a user to request remote access to the application server (p. 3, ll. 29-30), wherein the user enabling means includes a dialer having a dialing number associated therewith (p. 4, ll. 6-7);

a gaming card having security data for identifying the user (p. 16, ll. 17-19);

an access server (p. 3, l. 28), for receiving and processing a request for access to the application server (p. 3, ll. 27-29) from a user request enabling means, the server adapted to be located remote from the user's geographic location (p. 3, l. 30);

a card reader (p. 17, ll. 19-21) connected to the user enabling means at the user's geographic location (p. 17, ll. 21-24), wherein the card reader (p. 17, ll. 19-21) includes a time out feature (p. 17, ll. 21-24) that prompts the user to insert the gaming card into the card reader at an appropriate time to verify that the user is physically present at the user's geographic location;

an authenticator for authenticating the geographic location of the user responsive to receipt of the processed request from the access server (p. 3, l. 30 – p. 4, l. 1), the authenticator adapted to be connected to the access server (FIG. 1; p. 8, ll. 26-27), the authenticator including a Remote Access Dial-In Service (RADIUS) server (p. 4, ll. 7-8) and a challenge and response system (p. 4, ll. 19) for authenticating the geographic location of the user and verifying an identity of the user based on the security data (p. 4, l. 21), wherein the verifying the identity of the user includes issuing a challenge based on the security data (p. 10, ll. 6-12);

means for interconnecting the access server and the authenticator (FIG. 1; p. 4, l. 27);

a first number authenticating system (p. 9, l. 27- p. 10, l. 2), wherein the first number authenticating system provides anti-circumvention protection that determines a geographic location of an originating number to prevent the user from connecting to the access server from a geographic location other than the user's geographic location (p. 9, l. 27- p. 10, l. 2), and wherein the first number authenticating system relies on user input (p. 5, ll. 14-15; p. 17, ll. 13-14) and does not rely on GPS (p. 4, ll. 12-14).

Independent Claim 48:

A method of enabling remote access to an application server, the method comprising:

requesting an access server to enable a user to access an application server (p. 3, ll. 27-30);

authenticating a geographic location of the user via an authenticator, wherein the authenticator is connected to the access server (p. 3, l. 30 – p. 4, l. 1);

providing a time out feature via a card reader (p. 17, ll. 21-24), wherein the card reader is connected via a network to the access server (p. 4, ll. 1-3);

prompting the user to insert a game card into the card reader at an appropriate time to verify that the user is physically present at a user's geographic location (p. 16, ll. 21-24; p. 17, ll. 9-10);

authenticating an identity of the user based on the security data (p. 4, ll. 19-20), wherein the verifying the identity of the user includes issuing a challenge based on the security data via the authenticator (p. 10, ll. 6-12);

identifying a first number from which the user has dialed (p. 9, l. 27- p. 10, l. 2), wherein a first number authenticating system provides anti-circumvention protection that determines a geographic location of an originating number to prevent the user from connecting to the access server from a geographic location other than the user's geographic location (p. 9, l. 27- p. 10, l. 2), and wherein the first number authenticating system relies on user input (p. 5, ll. 14-15; p. 17, ll. 13-14) and does not rely on GPS (p. 4, ll. 12-14); and

determining in the authenticator whether to enable the user to access the application server based on the authenticating of the user's geographic location (p. 10, ll. 4-6).

(vi) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Examiner rejected claims 1, 2, 4-8, 10-21, 23, 24, 26-41, 43-49, 51-68, and 70-76 under 35 U.S.C. § 103(a) as being obvious over Goertzel in view of Shaffer.

The Examiner rejected claims 22, 25, and 69 under 35 U.S.C. § 103(a) as being obvious over Goertzel.

(vii) ARGUMENT

Claims 1, 2, 4-8, 10-21, 23, 24, 26-41, 43-49, 51-68, and 70-76 are not anticipated by Goertzel in view of Shaffer:

The Examiner rejected claims 1, 2, 4-8, 10-21, 23, 24, 26-41, 43-49, 51-68, and 70-76 under 35 U.S.C. § 103(a) as being obvious over Goertzel in view of Shaffer. Claims 4, 5, 10, 14, 17, 35-41, 43-47, 51, 56, 57, and 61 have been canceled, thereby rendering the rejection moot for those claims. The Applicants respectfully traverse the rejection of claims 1, 2, 4-8, 10-21, 23, 24, 26-41, 43-49, 51-68, and 70-76.

Independent claims 1 and 30 recite the following claim elements, not disclosed, taught, or suggested by either Goertzel or Shaffer, and not rendered obvious by Goertzel in view of Shaffer:

a gaming card having security data for identifying the user;

> a card reader ... wherein the card reader includes a time out feature that prompts the user to insert the gaming card into the card reader at an appropriate time to verify that the user is physically present at the user's geographic location;
>
> the authenticator including a challenge and response system for ... verifying an identity of the user based on the security data, wherein the verifying the identity of the user includes issuing a challenge based on the security data.

The "physical presence" claim element is supported in the Specification at least at p. 10, l. 27 – p. 33, l. 6. The "time out" claim element is supported in the Specification at least at p. 10, l. 28 – p.11, l. 17. The identity verification claim element is supported in the Specification at least at p. 10, ll. 5-18. The physical presence, time out, and identity verification elements have been added to independent claims 1, 30, and 48.

Goertzel's challenge and response authentication does not verify the physical presence of a user at the geographic location, does not provide a time out feature, and does not verify an identity of the user based on security data, wherein the security data is stored on a gaming card entered by the user in response to a prompting at an appropriate time. Goertzel discloses only one challenge and response embodiment of authentication—NTLM, based on the user's

password. Accordingly, a consumer may circumvent the NTLM by using a commercial software product, such as Norton pcAnywhere, to remotely enter the password (see Goertzel, 16:35-47). Further, because Goertzel's security issues are based on the logical[1] pathway of connection, not the geographical pathway of connection, Goertzel provides no incentive to verify the physical presence of the user. In fact, Goertzel discloses that,

> [a]s can be readily appreciated, as used herein, the term 'location' is a logical concept related to the type of location connection rather than a physical concept related to the distance from which the connection is originating.

(Goertzel, 5:12-15). "When the prior art teaches away from combining certain known elements, discovery of successful means of combining them is more likely to be nonobvious."[2] See also M.P.E.P. § 2144.05 entitled, Rebuttal Of Prima Facie Case Of Obviousness (stating that "a prima facie case of obviousness may also be rebutted by showing that the art, in any material respect, teaches away from the claimed invention").

Likewise, Shaffer does not disclose the claim elements of verifying the physical presence of a user at the geographic location, providing a time out feature, and verifying an identity of the user based on security data, wherein the security data is stored on a gaming card entered by the user in response to a prompting at an appropriate time. Although Shaffer teaches a relational database associating zip codes and telephone numbers, Shaffer does not overcome the shortcomings of Goertzel. Every Shaffer embodiment is directed to providing commercial services such as driving directions to local businesses (see Shaffer, 15:45-50). In stark contrast, the claimed elements are directed to preventing illegal transactions within a geographic location governed by a jurisdiction. With mutually exclusive goals, Shaffer provides no incentive to verify the physical presence of the user at the geographic location, as claimed. Therefore, the Applicants respectfully submit that claims 1, 2, 6-8, 11-21, 23, 24, 26-35, 37-41, 43-49, 52-55, 58-60, 62-68, and 70-76 are not obvious over Goertzel in view of Shaffer.

Claims 22, 25, and 69 are not obvious from Goertzel:

The Examiner rejected claims 22, 25, and 69 under 35 U.S.C. § 103(a) as being obvious

---

[1] *E.g.*, via remote access server (Goertzel, 5:46) or local intranet users (Goertzel, 6:54).

[2] *KSR Int'l Co. v. Teleflex Inc.*, 82 USPQ2d 1385, 1395 (2007).

over Goertzel. The Applicants respectfully traverse the rejection. The Applicants note that claims 22 and 25 depend from independent claim 1, and claim 69 depends from independent claim 48. The Applicants respectfully traverse the rejection of claims 22, 25, and 69.

As set forth in Section 3 of this Paper, the Applicants respectfully submit that independent claims 1 and 48 are not obvious over Goertzel. Therefore, at least by virtue of their dependence from claim 1, claims 22 and 25 are not obvious over Goertzel, and at least by virtue of its dependence from claim 48, claim 69 is not obvious over Goertzel.

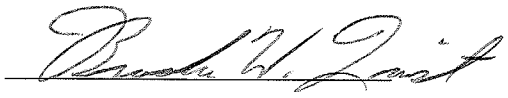
The shortcomings of Goertzel are well documented above with regard to the argument set forth for claims 1 and 48. As Goertzel does not disclose, teach, or suggest each and every limitation of independent claims 1 and 48 all of the respective dependent claims 22, 25, and 69 are not obvious from Goertzel.

CONCLUSION AND RELIEF

In conclusion, we respectfully request that the Board overturn the rejections of claims 1, 2, 4-8, 10-23, 24-41, 43-49, and 51-76 and hold claims 1, 2, 4-8, 10-23, 24-41, 43-49, and 51-76 allowable.

Respectfully submitted,

Date: September 22, 2008



BROOKE W. QUIST
REG. NO. 45,030
STEPTOE & JOHNSON LLP
2121 Avenue of the Stars
Suite 2800
Los Angeles, CA 90067
Tel 310.734.3200
Fax 310.734.3300

(viii) CLAIMS APPENDIX

The claims involved in this Appeal are as follows:

1. A system for enabling remote access to an application server, the system comprising:

a means for enabling a user to request remote access to the application server;

a gaming card having security data for identifying the user;

an access server, for receiving and processing a request for access to the application server from the means for enabling a user to request remote access to the application server, the access server adapted to be located remote from the user's geographic location;

a card reader connected to the means for enabling a user to request access to the application server at the user's geographic location, wherein the card reader includes a time out feature that prompts the user to insert the gaming card into the card reader at an appropriate time to verify that the user is physically present at the user's geographic location;

an authenticator for authenticating the geographic location of the user responsive to receipt of a processed request from the access server, the authenticator including a challenge and response system for authenticating the geographic location of the user and verifying an identity of the user based on the security data, wherein the verifying the identity of the user includes issuing a challenge based on the security data, and wherein the authenticator is adapted to be connected to the access server;

means for interconnecting the access server and the authenticator; and

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that determines a geographic location of an originating number to prevent the user from connecting to the access server from a geographic location other than the user's geographic location, and wherein the first number authenticating system relies on user input and does not rely on GPS.

2. The system of claim 1, wherein the authenticator comprises an authenticating server.

6. The system of claim 1, wherein the interconnecting means comprise a network.

7. The system of claim 2, wherein the authenticating server includes a database of authorized geographic locations, for enabling verification of the geographic location of the user as an authorized user geographic location.

8. The system of claim 2, wherein the authenticating server comprises a Remote Access Dial-In User Service (RADIUS) server.

11. The system of claim 1, wherein the means for enabling a user to request remote access to the application server includes an interface station.

12. The system of claim 1, wherein the means for enabling a user to request remote access to the application server includes a client.

13. The system of claim 1, wherein the means for enabling a user to request remote access to the application server includes a geographic location identifier.

15. The system of claim 1, wherein the means for enabling a user to request remote access to the application server includes an identifier associated with the user's geographic location, and the authenticator comprises means for authenticating the identifier associated with the user's geographic location.

16. The system of claim 1, wherein the means for enabling a user to request remote access to the application server includes a dialer located at the user's geographic location, and wherein the dialer includes a number associated therewith.

18. The system of claim 1, wherein the interconnecting means are further adapted to interconnect the means for enabling a user to request remote access to the application server.

19. The system of claim 6, wherein the network comprises an intranet.

20. The system of claim 6, wherein the network comprises the Internet.

21. The system of claim 8, further comprising means for enabling the user to request remote access to the application server, wherein the authenticating server is further adapted to issue a security challenge to the means for enabling a user to request remote access to the application server.

22. The system of claim 15, wherein the locating identifier comprises a cookie.

23. The system of claim 16, wherein the authenticator comprises a number identifier for identifying the number associated with the dialer located at the user's geographic location.

24. The system of claim 16, wherein a dialing system includes a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing therefrom and each dialer associated with a different user's geographic location, and the authenticator further comprises means for identifying the first number dialed from in the dialing system.

25. The system of claim 20, wherein the locating identifier comprises a dynamic cookie.

26. The system of claim 21, wherein the means for enabling a user to request remote access to the application server is adapted to issue a response to the security challenge, and the authenticator includes a database for enabling verification of the response of the means for enabling a user to request remote access to the application server to the security challenge.

27. The system of claim 23, wherein the number identifier comprises Automatic Number Identification.

28. The system of claim 24, wherein the first number identifying means comprises Dialed Number Identification Services.

29. The system of claim 26, wherein the authenticator is further adapted to verify the response of the means for enabling a user to request remote access to the application server to the security challenge based on the database in the authenticator, and to authorize access to the application server.

30. A system for enabling remote access to an application server, the system comprising:

a means for enabling a user to request remote access to the application server, wherein the user enabling means includes a dialer having a dialing number associated therewith;

a gaming card having security data for identifying the user;

an access server, for receiving and processing a request for access to the application server from a user request enabling means, the server adapted to be located remote from the user's geographic location;

a card reader connected to the user enabling means at the user's geographic location, wherein the card reader includes a time out feature that prompts the user to insert the gaming card into the card reader at an appropriate time to verify that the user is physically present at the

user's geographic location;

an authenticator for authenticating the geographic location of the user responsive to receipt of the processed request from the access server, the authenticator adapted to be connected to the access server, the authenticator including a Remote Access Dial-In Service (RADIUS) server and a challenge and response system for authenticating the geographic location of the user and verifying an identity of the user based on the security data, wherein the verifying the identity of the user includes issuing a challenge based on the security data;

means for interconnecting the access server and the authenticator;

a first number authenticating system, wherein the first number authenticating system provides anti-circumvention protection that determines a geographic location of an originating number to prevent the user from connecting to the access server from a geographic location other than the user's geographic location, and wherein the first number authenticating system relies on user input and does not rely on GPS.

31. The system of claim 30, wherein the authenticator includes a number identifier for identifying the number associated with the dialer located at the user's geographic location.

32. The system of claim 30, and further comprising a dialing system including a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing therefrom and each associated with a different user's geographic location, and the authenticator comprises means for identifying the first number dialed from the dialing system.

33. The system of claim 31, wherein the number identifier comprises Automatic Number Identification.

34. The system of claim 32 wherein the first number identifying means comprises Dialed Number Identification Services.

48. A method of enabling remote access to an application server, the method comprising:

requesting an access server to enable a user to access an application server;

authenticating a geographic location of the user via an authenticator, wherein the authenticator is connected to the access server;

providing a time out feature via a card reader, wherein the card reader is connected via a

network to the access server;

prompting the user to insert a game card into the card reader at an appropriate time to verify that the user is physically present at a user's geographic location;

authenticating an identity of the user based on the security data, wherein the verifying the identity of the user includes issuing a challenge based on the security data via the authenticator;

identifying a first number from which the user has dialed, wherein a first number authenticating system provides anti-circumvention protection that determines a geographic location of an originating number to prevent the user from connecting to the access server from a geographic location other than the user's geographic location, and wherein the first number authenticating system relies on user input and does not rely on GPS; and

determining in the authenticator whether to enable the user to access the application server based on the authenticating of the user's geographic location.

49. The method of claim 48, wherein the authenticator comprises an authenticating server, and wherein authenticating further comprises authenticating through the authenticating server.

52. The method of claim 48, further comprising enabling the user to request remote access to the application server through the user request enabling means.

53. The method of claim 48, further comprising interconnecting the access server and the authenticating means through a network.

54. The method of claim 49, wherein authenticating the geographic location comprises authenticating through an authorized geographic location database.

55. The method of claim 49, wherein authenticating the geographic location further comprises authenticating through a RADIUS server.

58. The method of claim 52, wherein enabling further comprises enabling the user request through an interface station.

59. The method of claim 52, wherein enabling further comprises enabling the user request through a client.

60. The method of claim 52, wherein enabling further comprises enabling the user request through the geographic location identifier.

62. The method of claim 52, wherein authenticating the geographic location comprises authenticating the user's geographic location through a user associated identifier.

63. The method of claim 52, wherein enabling comprises enabling through a dialer having an associated number.

64. The method of claim 52, wherein interconnecting comprises interconnecting a plurality of user request enabling means through a plurality of local area networks.

65. The method of claim 52, wherein interconnecting further comprises interconnecting with a user request enabling means.

66. The method of claim 53, wherein the network comprises an intranet, and wherein interconnecting further comprises interconnecting through the intranet.

67. The method of claim 53, wherein the network comprises the Internet, and wherein interconnecting further comprises interconnecting through the Internet.

68. The method of claim 55, wherein authenticating the identity of the user further comprises issuing a security challenge to the user request enabling means through an authenticating server.

69. The method of claim 62, wherein authenticating the geographic location further comprises authenticating through a locating identifier cookie.

70. The method of claim 63, wherein the authenticator comprises means for identifying the number associated with the dialer located at the user's geographic location, and wherein the step of authenticating the geographic location further comprises identifying the number associated with the dialer.

71. The method of claim 63 wherein a dialing system includes a plurality of numbers each associated with one of a plurality of dialers adapted to enable dialing therefrom and each associated with a different user geographic location, and the authenticator comprises means for identifying the first number dialed in the dialing system, and wherein the step of authenticating further comprises identifying the first number dialed.

72. The method of claim 67, wherein the locating identifier comprises a dynamic cookie.

73. The method of claim 68, wherein the user request enabling means are adapted to

issue a response to the security challenge, and the authenticator include a database for enabling verification of the response of the user request enabling means to the security challenge, and wherein the step of authenticating further comprises verifying the response to the security challenge through the verification database.

74. The method of claim 70, wherein identifying further comprises identifying through Automatic Number Identification.

75. The method of claim 71, wherein the step of identifying further comprises identifying through Dialed Number Identification Services.

76. The method of claim 73, wherein the authenticator is further adapted to verify the response of the user request enabling means to the security challenge based on the database in the authenticator, and to authorize access to the application server, and further comprising the step of authorizing access to an application server.

(ix) EVIDENCE APPENDIX

No evidence has been submitted pursuant to §§ 1.130, 1.131, or 1.132 of this title. No other evidence has been entered by the examiner and relied upon by appellant in the appeal.

(x) RELATED PROCEEDINGS APPENDIX

As there are no prior or pending appeals, interferences, or judicial proceedings known to the appellant, the appellant's legal representative, or the assignee which may be related to, directly affect, or be directly affected by, or have a bearing on the Board's decision in this pending appeal (pursuant to 37 CFR § 41.37(c)(1)(ii)), there are no decisions rendered by a court or the Board in any proceedings to include herein.